International Journal of Mechanical and Production Engineering Research and Development (IJMPERD)
ISSN(P): 2249-6890; ISSN(E): 2249-8001
Vol. 7, Issue 1, Feb 2017, 41-52

TRANS STELLAR
•Journal Publications •Research Consultancy

ROBUST AND SECURE PIXEL DOMAIN DIGITAL IMAGE STEGANOGRAPHY

ANU BINNY[1] & KOILAKUNTLA MADDULETY[2]

[1]*Research Scholar (Electronics), Dr. K .N. Modi University, Niwai, Rajasthan, India*

[2]*Associate Professor (Operations Management), National Institute of Industrial Engineering (NITIE), Mumbai, India*

ABSTRACT

Steganography is used in various information hiding applications which encodes the secret data by hiding the existence of the information so that a viewer cannot identify the presence of the secret message. A data securing technique is proposed for embedding the information bits in color images (RGB planes). The input cover image is divided into separate R, G and B planes and then the secret data is embedded. For embedding and extraction, sequential and pseudo random encoding and decoding technique is employed. The randomization process during the encoding adds more security to the method. Experimental results are performed using USC-SIPI image database. Various performance evaluation parameters like PSNR, RMSE and SNR are computed in order to prove the better performance of the presented algorithm. Experimental results demonstrate that the proposed algorithm outperforms all the existing data embedding algorithms in terms of PSNR values

KEYWORDS: Steganography, Sequential Encoding, Randomization and Encryption

Received: Dec 26, 2016; **Accepted:** Jan 21, 2017; **Published:** Jan 31, 2017; **Paper Id:** IJMPERDFEB20175

Original Article

INTRODUCTION

Due to tremendous development of computer hardware, software and network technology, one can easily transmit or receive secret information in different forms over the entire globe using the Internet. Large information content is transmitted and received over the Internet every day. In case of important secret data being exchanged over some unreliable public channel, there is a danger of leaking of the secret data. Information hiding and steganography is most popular since time immemorial for secret communication.

The word steganography is derived from the Greek words stegos means cover and grafia means writing [1].

The secure information transmission is achieved using steganography. Based on the cover, steganography can be classified into various types. In image steganography the information is hidden in images, whereas in audio steganography secret information is present. Steganography is an art of hiding written data or messages.

Steganography and cryptography are two separate fields. Cryptography makes the secret message undetectable without a key. The original medium can be referred to as cover .It may be text, image, audio or video. The secret data embedded is called as payload. The cover after embedding secret data is referred to as stego medium. A stego-key is used for hiding/encoding process to restrict detection or extraction of the embedded data [2].

Based on the cover medium, steganography can be classified into five types: (1) Text Steganography (2) Image Steganography (3) Audio Steganography (4) Video Steganography (5) Protocol Steganography.

Text steganography is the most common type of steganography used for hiding secret message in text message. It is not popular as embedding capacity of text files is very small. In image steganography, images are used as the cover medium for embedding secret data. A message is inserted into a digital image using an embedding algorithm and the secret key. At the receiver end, secret message is recovered using the extraction algorithm and the same key. Audio medium is used in audio steganography for embedding information. Currently, audio steganography algorithms can embed messages in WAV and MP3 files. Various widely used audio steganography methods are: LSB coding, Phase coding, Spread spectrum and Echo hiding. Video files can also be used for hiding secret data in Video Steganography. Protocol steganography is employed to embed messages within network protocols such as TCP/IP.

GENERAL MODEL OF STEGANOGRAPHY

Figure 1 shows the general model of a steganography system. In this model, image cover medium is used and the stego image is obtained by embedding the with the encryption key.

Compression and encryption processes eliminate the redundancy in secret message and in turn result in enhanced security.

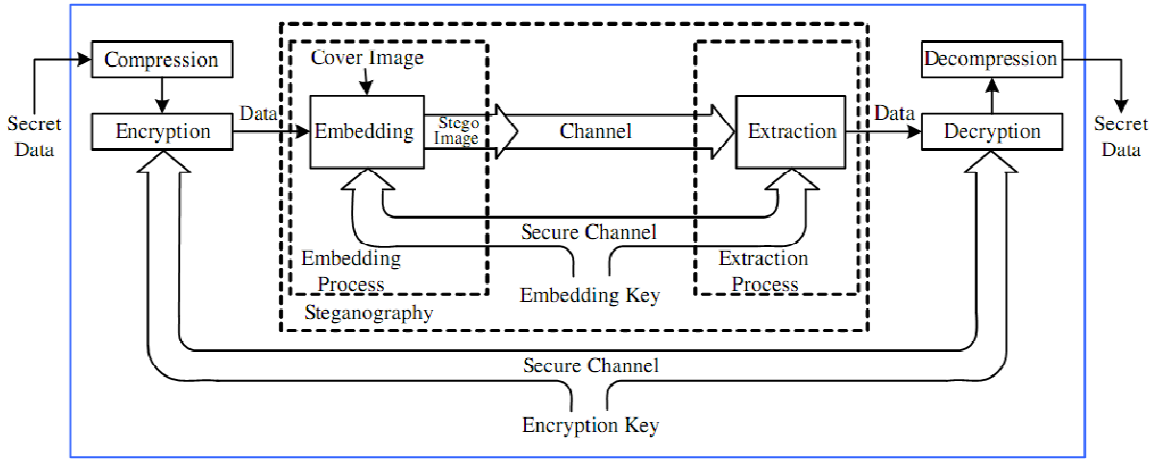

Figure 1: General Model of Steganography [3]

Applications of Steganography

- **Secret Communications:** For secure transmission and reception of information without knowing the attackers.
- **Copyright Protection:** The protection mechanisms to prevent copying of digital data by inserting watermarks.

In this paper, LSB substitution based on sequential encoding and Pseudo random encoding image steganography algorithm is proposed. First, the cover image is selected for embedding based on contrast criterion. Rest of the paper is organized as follows: Section II discusses the literature survey on various image steganography schemes. Section III describes the data embedding and extraction process. Section IV presents the proposed steganography algorithm. Section V demonstrates the experimental results and discussions. Finally Section VI concludes the paper.

Related Work

The basic idea behind the image steganography is to embed the secrete message into the image which is sent over unreliable public network. In this section, various image steganography schemes are discussed. Image steganography

algorithms are classified into (a) spatial domain, (b) transform domain, (c) spread spectrum and (4) model based steganography.

Spatial Domain Steganography

In this approach, the secret data is embedded in modifying the pixel values.

In the LSB embedding approach, embedding is done by replacing selected cover image pixels by the secret data.

Main advantages of special domain methods are that they include more hiding capacity and they are easy to implement. Many steganographic tools based on LSB substitution method are available like StegHide, S tool, Stegnos etc. In [4], LSB based data hiding schemes are proposed. Best example is the Adaptive LSB substitution based on brightness, edges and texture masking of the host image. Other LSB methods are lossless generalized LSB data embedding [5], optimized LSB substitution using cat swarm strategy and genetic algorithm [6]-[7], data hiding based on histogram modification [8].

In [9], information message bits are embedded in multiple bit planes using multi bit steganography. Gray level modification technique is used to map the secret data using the gray levels of pixels based on some mathematical function [10]. Advantage of this method was low complexity and large data hiding capacity. An embedding method is proposed by Wu and Tsai based on the difference between pixel values [11]. First, the cover image is divided into identical non overlapping blocks and the difference in each block is modified. Greater modification is possible in case of large difference values. Another method based on PVD is PVD method vulnerable to histogram analysis [12], tri- way PVD and four-way PVD [13]-[15].

Singular value decomposition (SVD) and vector quantization is employed to embed the data, resulting in better image quality [16]. This approach is outperformed by the method proposed in [17] using reversible data hiding scheme for VQ indices. A hybrid steganography scheme is proposed using Noise Visibility Function (NVF) and an optimal chaotic based encryption scheme in [18]. The optimal chaotic based encryption scheme is achieved by using a hybrid optimization of Particle Swarm Optimization (PSO) and Genetic Algorithm (GA) used to identify an optimal secret key.

Frequency Domain Steganography

In transform domain steganography the secret message is embedded in the transform coefficients of the cover image. Discrete Cosine Transform and Discrete Wavelet Transform are examples of most popular transform domain. The transform domain methods are more resistive to attacks and are used to minimize redundancy and to locate less important parts of image.

In [19], Eigen values of quantized DCT matrices are used for embedding the secret data. The technique has higher embedding and hence, robust against Subtractive Pixel Adjacency Matrix (SPAM) steganalyzer. Mali et al. [20] proposed DCT coefficients and interleaving and randomization spreads the embedded information all over the cover image using Class Dependent Coding Scheme (CDCS).

Image Steganography is presented using DCT coefficients. Similarities between the adjacent image blocks which preserve good image quality as embedding distortion is spread within the image blocks are presented[21]. In [22], middle-frequency components of the quantized DCT coefficients resulted in larger hiding capacity with acceptable image quality using modified quantization table. Where as in [23] Solanki et al, coefficients that lie in a low frequency band of 21

coefficients for data embedding are used.

In [24], an algorithm for image steganography is presented using successive zero coefficients of the medium-high frequency components in each reconstructed block for three-level DWT of a cover image. Embedding in lifting based discrete wavelet transform (DWT) coefficients instead of conventional DWT is performed in [25]. Liu et al [26] presented an image steganography algorithm by dividing whole JPEG 2000 bit stream into multiple layers where every layer is of 0.5 bpp and backward embedding was performed in each layer. Major advantages of the method are high embedding capacity, progressive extractability and better image quality. Using significant wavelet coefficients and their texture and sensitivity to gray value variations, the positions and the magnitudes are opted to adaptively embed the secret message in [27].

A frequency domain steganography approach based on Fresnelet transform (FT) is proposed in [28]. In this method, the Fresnelet coefficients of the Least Significant Bit (LSB) at high frequency sub-bands are used to embed the QR coded secret message.

PROPOSED SCHEME FOR EMBEDDING AND EXTRACTION

The least significant bit (LSB) of the bytes from an image is changed to a bit of the secret information bits. Digital images are primarily of two types (i) Color or 24 bit images and (ii) gray or 8 bit images. In color images, three bits of secret message can be embedded in each pixel. Changing the bit position from 0 to 1 or from 1 to 0 using the LSB does not change the visual appearance of the image and hence output stego looks like the cover image.

In gray scale images, one bit of secret data can be embedded.

If the LSB of the pixel value of cover image X(u,v) is equal to the message bit m of secret data to be embedded, X(u,v) remain unaltered. Else, the LSB of C(i, j) changes with changes in m. The information embedding procedure can be explained below:

$S(i,j) = X(u,v) - 1$, if $LSB(X(u,v)) = 1$ and $m = 0$

$S(i.j) = X(u,v)$, if $LSB(X(u,v)) = m$

$S(i,j) = X(u,v) + 1$, if $LSB(X(u,v)) = 0$ and $m = 1$

where $LSB(X(u,v))$ represents the LSB of cover image $X(u,v)$ and m is the information bit to be embedded and

$S(i,j)$ is the stego image.

In the proposed method, information bit embedding is performed using sequential encoding and decoding and using pseudo random encoding and decoding approach.

Figure 2 Shows the Generalized Block Diagram of the Proposed Steganography Algorithm. Detailed Description of The Schematic is presented in This Section.

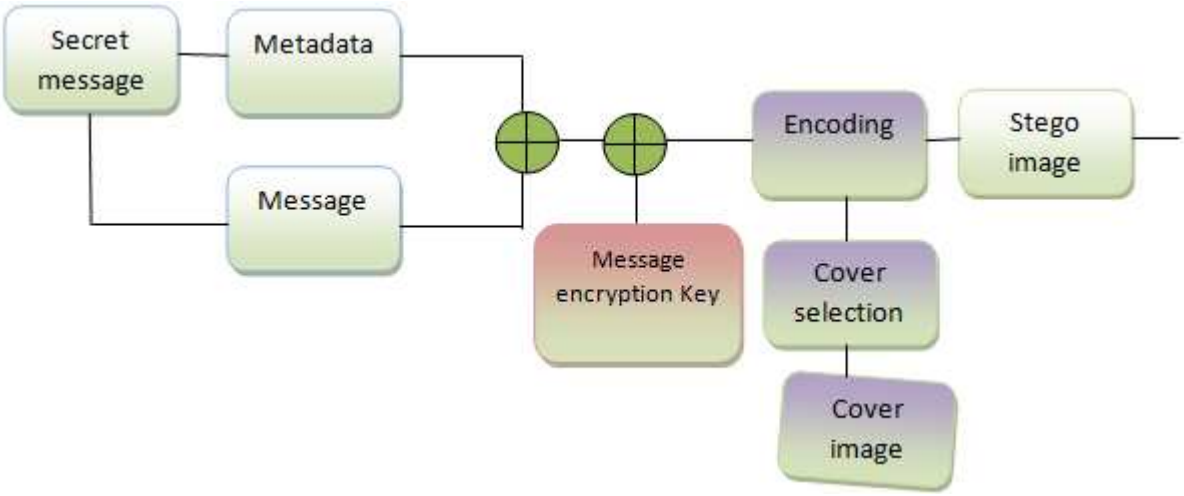

Figure 2: Generalized Block Schematic of Data Embedding Algorithm

Image Steganography using Sequential Encoding and Decoding Approach

The main objective of steganography is to embed the information into the carrier in an imperceptible way to hide the secret data. Two important considerations during any steganographic algorithm development are the embedding capacity and imperceptibility of the data in stego image. In addition to this, cover image selection for embedding the secret information is also important. Various cover selection methods are proposed in literature, for example, correlation parameter, JPEG quality factor, Bhattacharya distance, contrast and similarity. In this experiment, we have employed contrast based cover image selection. Using co occurrence matrix, contrast value is computed. Higher contrast values results in better cover image selection which hides the presence of the secret data. Hence, images with higher contrast value are chosen out of the large image database as the cover image.

Input secret information bits are converted into an integer bit stream before the embedding process. In the present work, as the input secret data is in text form, the input bit stream is formed by simply converting the ASCII code of each character into an 8-bit binary code. After the contrast based cover selection process, the sequential encoding function is performed on the cover images. The input cover image is color (RGB) which consists of three colour planes. Hence the sequential encoding is done on each colour plane separately.

The type of message and information about its length is encoded in the message. Encoding further sequentially encodes the message values across the RGB channels in RGBBGRGR order. The input message encodes from the top to bottom and left to right. In addition to this, the encoding algorithm uses a secured encryption key.

Embedding Scheme

Step 1: Read the Input cover in the color RGB format.

Step 2: Apply contrast based cover image selection for selecting cover image.

Step 3: Get all the details (type of message and message length) of message

Step 4: Read secret information bits and convert it into integer values

Step 5: Select the input encryption key for data embedding

Step 6: Encrypt the secret message (integer form) using symmetric XOR encryption key

Step 7: The encrypted data is embedded in cover image using sequential encoding scheme i.e. hideing the data along the columns moving from left to right.

Step 8: Generate stego image consisting of message.

At the receiver side, the secret information is extracted using the decoding process from the stego images.

In addition to this, the encryption key which is used at the encoding process is shared by the decoder algorithm to retrieve the hidden text in stego image. The decoder algorithm receives the stego image, and after decoding the header, information like type of message and length of message is extracted. Finally the decoder sequentially decodes the data and the secret message is recovered. The detailed steps are given below:

Extraction Scheme

Step 1: Select the input RGB stego image

Step 2: Extract header and obtain type and length of the message

Step 3: Extract RGB components separately

Step 4: Input encryption key (Same as the encoder)

Step 5: Decrypt the input data using XOR encryption key which is shared with encoder

Step 6: Apply reverse order steps using modulo arithmetic to extract hidden data.

Step 7: Store the extracted message bits

Image Steganography using Pseudo Random Encoding and Decoding Approach

Image pixels are selected randomly for information embedding in pseudo random encoding approach. Message bits are embedded in the LSB of a different colour plane of the randomly selected pixels.

Embedding Algorithm

In the embedding process, a random key is applied to randomized the input cover image. Next, the secret information bits are embedded into the least significant bit of the pixels. The encoder and decoders share the random-key. The random-key is generated using a pseudo-random number generator. The detailed procedure for embedding the message using pseudo random encoding technique is summarized as:

Step 1: Read the characters from input text file (message to be hidden) and convert into an 8 bit integer array.

Step 2: Get the input color image in RGB format which is called as cover image.

Step 3: Read the MSB of the pixel and initialize the random key

Step 4: Cover image pixels are randomly reshaped into a matrix using green channel.

Step 5: Get the stego-key and XOR with text file of secret message.

Step 6: Replace the LSB of the cover image with the bits of the secret information

Step 7: Store the stego image.

Extraction Algorithm

The random key is required which is same as encoder to extract the LSB where the secret message is randomly distributed. Extraction algorithm identifies the secret bits into LSB of the pixels within a cover image using the random key distributed. Detailed procedure can be summarized as follows:

Step 1: Read the input stego image.

Step 2: Extract the red component of the host image.

Step 3: Read the last bit of each green channel pixel.

Step 4: Input the random-key by using which the position of the random hidden bits can be identified in the given image.

Step 5: Extract the pixels based on random key

Step 6: Obtain the least significant bit of green pixel.

Step 7: Get ASCII value of each character from the hidden message bits.

Step 8: X-OR these ASCII values with shared stego-key resulting in original message hidden at the encoder.

EXPERIMENTAL RESULTS AND DISCUSSIONS

This section presents the experimental result of the proposed method. The algorithm is evaluated using color images of size 512 X 512 [USC-SIPI from USC-SIPI image database. All the simulations were carried out using MATLAB 2012a with Core i-3 Processor, 2 GB RAM and Windows 7 operating system. Sample test images from the database and corresponding stego images are shown in figure 3

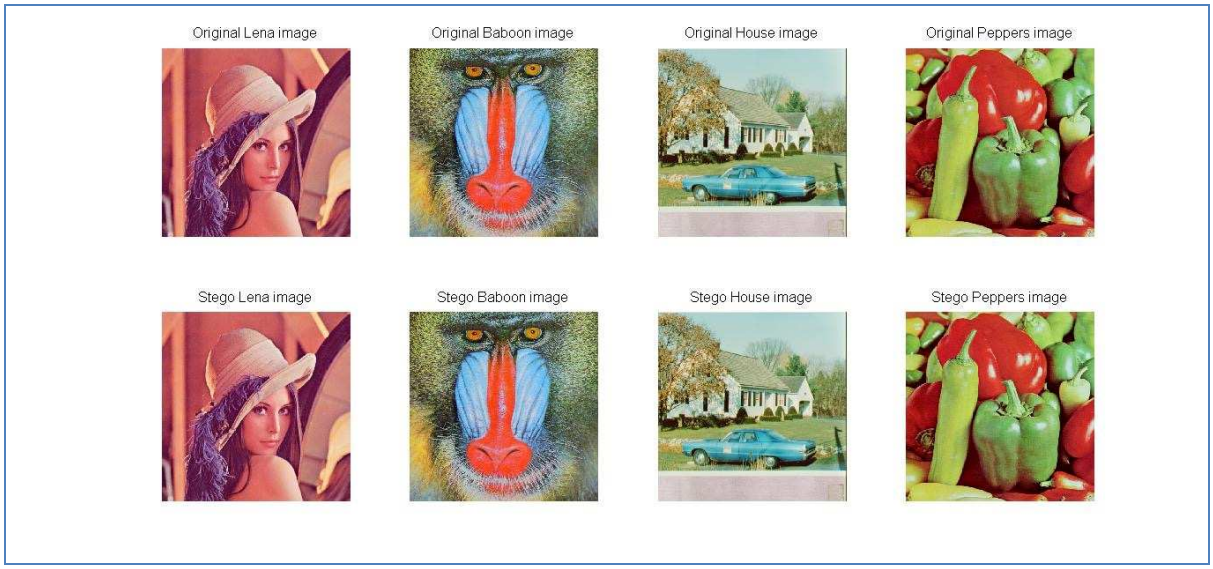

Figure 3: Original Test Images and Corresponding Stego Images. First Row Shows Original Images and Second Row Shows Stego Images

The proposed algorithm hides effectively the secret information bits with minimum visual distortion into the cover image and extracts it efficiently at the decoder side. The resulting stego image has good visual quality i.e. higher PSNR. Various parameters like PSNR, RMSE and SNR are computed to measure the performance of the proposed

algorithm. These parameters are computed as,

- Root Mean Square Error (RMSE): (01)

  Where $N \times M$ = Image size, I_{ij}= Cover image, $\tilde{I}_{ij}$ =Stego image

- Peak Signal to Noise Ratio (*PSNR*) (02)

- Signal to Noise Ratio (SNR) (03)

  Where $f(x, y)$ = Cover image and $\tilde{f}(x, y)$ = Stego image

Table 1 shows PSNR, RMSE and SNR of various images from USC-SIPI image database using sequential encoding and decoding algorithm. Images are embedded with different size of secret information bits. In this experiment we use 1k, 10k and 20k of text file size.

Table 1: PSNR, RMSE and SNR Parameters using Sequential Encoding and Decoding

Image	SNR (dB)			RMSE			PSNR (dB)		
	1K	10K	20K	1K	10K	20K	1K	10K	20K
Lena	61.58	51.47	47.79	0.054	0.168	0.238	73.26	63.68	60.65
House	62.45	53.68	43.51	0.057	0.120	0.198	74.04	65.58	61.01
Peppers	58.92	49.93	40.27	0.048	0.107	0.178	74.76	66	62.38
Baboon	60.81	51.46	42.38	0.052	0.110	0.189	73.81	64.13	60.26

Table 2: PSNR, RMSE and SNR Parameters using Pseudo Random Encoding and Decoding

Image	SNR (dB)			RMSE			PSNR (dB)		
	1K	10K	20K	1K	10K	20K	1K	10K	20K
Lena	62.49	53.28	46.10	0.053	0.157	0.215	73.62	64.25	61.84
House	61.94	52.12	42.82	0.052	0.132	0.201	73.16	65.21	60.92
Peppers	58.72	48.27	41.10	0.051	0.129	0.219	73.93	66.29	61.85
Baboon	60.42	50.97	42.12	0.052	0.117	0.194	73.79	63.69	61.02

From Tables 1 and 2 it is evident that, PSNR values are higher even in case of high information embedding resulting in better quality stego images. It is also observed that, sequential encoding and decoding performs better compared to pseudo random encoding and decoding at higher secret data embedding. Higher SNR and lower RMSE values indicate better performance of the proposed algorithm.

Some of the existing algorithms shows changes in the stego image histogram compared to original image histograms indicating the presence of data hiding. In this simulation, experiments are performed to verify the effect of data embedding on stego image histogram. Figure 4 shows

Also, RGB histogram of both original and stego images is plotted in figure has been plotted as shown in figure 4 and 5 when 10K sret data was embedded. Figure 4 shows RGB histograms of original and stego images using Lena and Baboon images. Figure 5 shows RGB histograms of original and stego images using House and Peppers images. Both the histograms are almost same, indicating both images have similar characteristics and it is difficult to identify the presence of secret data.

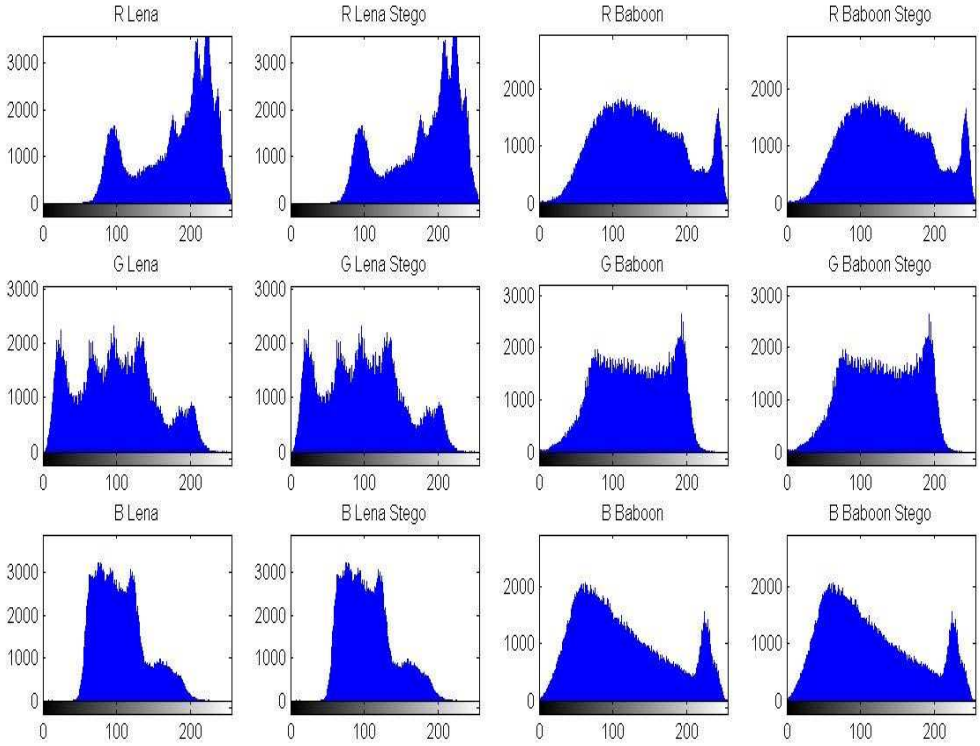

Figure 4: RGB Histograms of Original and Stego Images. (a) First Column: RGB Histograms of Original Lena Image (b) Second Column: RGB Histograms of Stego LENA Image (c) Third Column: RGB Histograms of Original Baboon Image (d) Fourth Column: RGB Histograms of Stego Baboon Image

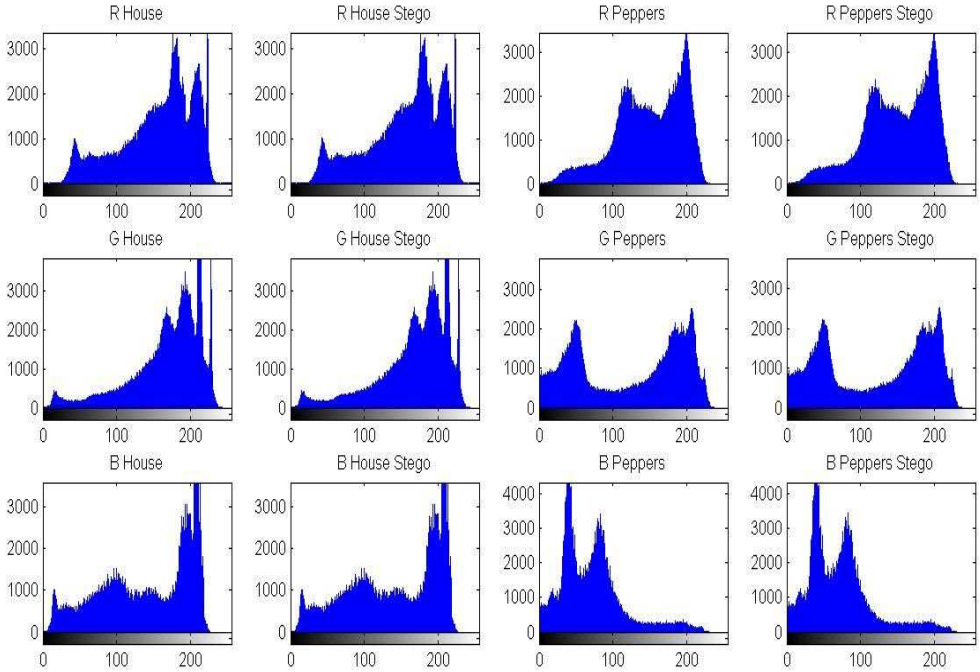

Figure 5: RGB Histograms of Original and Stego Images. (a) First Column: RGB Histograms of Original House Image (b) Second Column: RGB Histograms of Stego House Image (c) Third Column: RGB Histograms of Original Peppers Image (d) Fourth Column: RGB Histograms of Stego Peppers Image

Figure 6 shows difference image (difference between original and stego image) where white pixels indicate the presence of spatial locations.

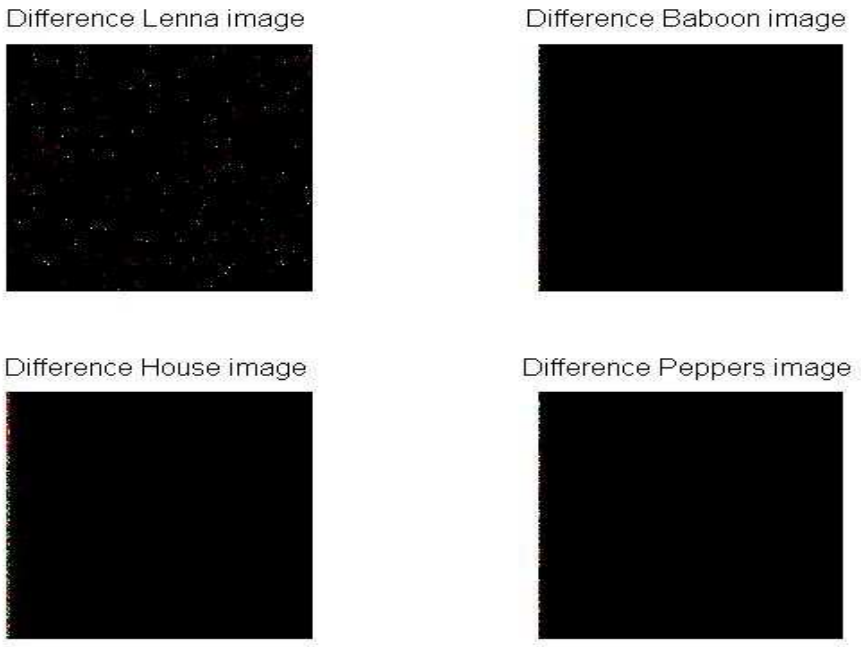

Figure 6

Proposed algorithm is compared with few existing methods in table 3.

Table 3

Algorithm	PSNR (dB)
[29]	71.28
[30]	46
[31]	56.78
Proposed	74.04

CONCLUSIONS

Steganography is an important field in information hiding which refers to the technique of hiding secret data into digital images without having any attention. The proposed work is focused on efficient steganographic approach using sequential and pseudo random encoding decoding. The algorithm is applied over USC-SIPI image database for evaluation. PSNR, SNR and RMSE parameters are computed to measure the performance of the presented approach. Experimental results demonstrate that the presented method performs better compared to other existing algorithms. In future, algorithm presented can be modified to employ other multimedia cover source (audio and video).

REFERENCES

1. *R.Anderson and F. Petitcolas, "On the limits of steganography" IEEE Journal of Selected Areas in Communications, Vol. 16, No. 4, May 1998.*
2. *Niels Provos, Peter Honeyman, "Hide and Seek: An Introduction to Steganography," IEEE computer society,2003.*
3. *V. Sabeti, S. Samavi, M. Mahdavi, S. Shirani, Steganalysis and payload estimation of embedding in pixel differences using neural networks, Pattern Recognit. 43 (2010) 405–415.*

4. *Hengfu YANG, Xingming SUN, Guang SUN, "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution", Radio Engineering, Vol. 18, No. 4, pp 509-516 December 2009*
5. *Mehmet Utku Celik, Gaurav Sharma, Ahmet Murat Tekalp and Eli Saber, "Lossless Generalized-LSB Data Embedding", IEEE transactions on image processing, Vol. 14, NO. 2, pp 253-266, February 2005*
6. *Zhi-Hui Wang, Chin-Chen Chang, Ming-Chu Li, "Optimizing least-significant-bit substitution using cat swarm optimization strategy", Information Sciences (192), pp.98–108,2012*
7. *Shen Wang, Bian Yang and Xiamu Niu, "A Secure Steganography Method based on Genetic Algorithm", Journal of Information Hiding and Multimedia Signal Processing .Vol.1, No.1, pp 28-35, January 2010*
8. *Zhenfei Zhaoa, Hao Luoc, Zhe-Ming Luc, Jeng-Shyang Pand, " Reversible data hiding based on multilevel histogram modification and sequential recovery", Int. J. Electron. Communication, pp. 814- 826, 2011*
9. *B. Cong, N. Sang, M. Yoon, H.-K. Lee, Multi bit plane image steganography, in: International Workshop on Digital forensics and Watermarking, vol. 4283 of Lecture Notes in Computer Science, pp. 61–70.*
10. *V.M. Potdar, E. Chang, Gray level modification steganography for secret communication, in: Proc. of 2nd IEEE International Conference on Industrial Informatics, pp. 223–228.*
11. *D. Wu, W.H. Tsai, A steganographic method for images by pixel value differencing, Pattern Recognit. Lett. 24 (2003) 1613–1626.*
12. *X. Zhang, S. Wang, Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security, Pattern Recognit. Lett. 25 (2004) 331–339.*
13. *C.-H. Yang, C.-Y. Weng, H.-K. Tso, S.-J. Wang, A data hiding scheme using the varieties of pixel-value differencing in multimedia images, J. Syst. Softw. 84 (2011) 669–678.*
14. *Y.-P. Lee, J.-C. Lee, W.-K. Chen, K.-C. Chang, I.-J. Su, C.-P. Chang, High-payload image hiding with quality recovery using tri-way pixel-value differencing, Inform. Sci. 191 (2012) 214–225.*
15. *X. Liao, Q. yan Wen, J. Zhang, A steganographic method for digital images with four-pixel differencing and modified LSB substitution, J. Vis. Commun. Image Represent. 22 (2011) 1–8.*
16. *K.L. Chung, C.H. Shen, L.C. Chang, A novel SVD and VQ based image hiding scheme, Pattern Recognit. Lett. 22 (2001) 1051–1058.*
17. *C.-C. Chang, T.S. Nguyen, C.-C. Lin, A reversible data hiding scheme for VQ indices using locally adaptive coding, J. Vis. Commun. Image Represent. 22 (2011) 664–672.*
18. *S. Sajasi, A.-M.E. Moghadam, An adaptive image steganographic scheme based on Noise Visibility Function and an optimal chaotic based encryption method, Applied Soft Computing Journal, Vol.30, pp.375-389, 2015.*
19. *Yasser M. Behbahani, Parham Ghayour, Amir Hossein Farzaneh, "Steganography Based on Eigen Characteristics of Quantized DCT Matrices", Proceedings of the 5th International conference on IT & Multimedia at UNITEN Malaysia, pp. 1-4, November 2011*
20. *Suresh N. Mali, Pradeep M. Patil, Rajesh M. Jalnekar, " Robust and secured image-adaptive data hiding", Digital Signal Processing, Vol.22Issue2,pp.314-323,March2012*
21. *Rufeng Chu, Xinggang You, Xtangwei Kong, Xiaohui Ba, "A DCT-based image steganographic method resisting statistical attacks", IEEE International Conference on Acoustics, Speech, and Signal Processing, Vol.5 . pp 953-956, May 2004*

22. *Chen Chang,T ung-Shou Chen, Lou-Zo Chung Chin . " A steganographic method based upon JPEG and quantization table modification", Information Sciences (141), pp.123-13,2008*

23. *Solanki, K. Sullivan, K. Madhow, U. Manjunath, B.S., Chandrasekaran, S. "Provably Secure Steganography: Achieving Zero K-L Divergence using Statistical Restoration" , IEEE International Conference on Image Processing, pp.125-128, Oct. 2006*

24. *Hui-Yu Huang, Yunlin, Taiwan, Shih-Hsu Chang, "A 9/7 wavelet-based lossless data hiding", IEEE Symposium on Computational Intelligence for Multimedia, Signal and Vision Processing (CIMSIVP), pp.1-6, April 2011.*

25. *Amit Phadikar, Santi P. Maity, "Data hiding based quality access control of digital images using adaptive QIM and lifting", Journal of Signal Processing: Image Communication, Vol. 26, Issue 10, pp.646-661, November 2011*

26. *Wei Liu, "Data hiding in JPEG2000 code streams", International conference on Image Processing (ICIP), pp. 1557-1560,2004*

27. *Youssef, S.M. Elfarag, A.A. Raouf, R., "C7. A multi-level information hiding integrating wavelet-based texture analysis of block partition difference images", 29th National Radio Science Conference (NRSC), pp. 203-210, April 2012*

28. *Uma Maheswari and D. Jude Hemanth. Frequency domain QR code based image steganography using Fresnelet transforms. International Journal of Electronics and Communications (AEÜ), 69 (2015) 539–544.*